

AO 106 (Rev. 04/010) Application for Search Warrant

AUTHORIZED AND APPROVED/DATE:

## UNITED STATES DISTRICT COURT

WESTERN

for the  
DISTRICT OF

OKLAHOMA

In the Matter of the Search of )

PREMISES KNOWN AS )

1111 S. Ellison Street,  
Guymon, Oklahoma 73942 )

Case No: M-21-490-SM

## APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

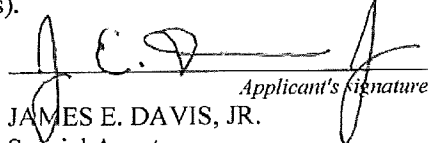
*Code Section*  
 18 USC § 2252A(a)(5)(B) and 2252A(a)(2)

*Offense Description*  
 Possession and distribution of child pornography

The application is based on these facts:

See attached Affidavit of Special Agent James E. Davis, Jr., Homeland Security Investigations, which is incorporated by reference herein.


- ☐ Continued on the attached sheet(s).  
☐ Delayed notice of \_\_\_\_\_ days (*give exact ending date if more than 30 days*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

  
 Applicant's signature  
 JAMES E. DAVIS, JR.  
 Special Agent  
 Homeland Security Investigations

Sworn to before me and signed in my presence.

Date: August 18, 2021

City and State: Oklahoma City, Oklahoma

  
 Judge's signature  
 SUZANNE MITCHELL, U.S. Magistrate Judge  
 Printed name and title

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, James E. Davis Jr., a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I have been employed as a Special Agent (“SA”) of the U.S. Department of Homeland Security, Homeland Security Investigations (“HSI”), since 2020 and have been employed as a federal investigator since 2015. I am currently assigned to HSI Amarillo, Texas. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I received training at the Federal Law Enforcement Training Center and have gained experience through prior investigations involving child exploitation, including the possession, distribution, and/or production of child pornography. I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media including, but not limited to, computer media. I have access to the institutional knowledge developed around this type of investigation by working with other experienced child exploitation criminal investigators and non-profit organizations. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the entire property located at 1111

S. Ellison Street, Guymon, Oklahoma, 73942 (the “SUBJECT PREMISES”), the content of electronic storage devices located therein, and any person located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of 18 USC §§ 2252A(a)(5)(B) and 2252A(a)(2) (Possession and distribution of child pornography, respectively). These items are more specifically described in **Attachment B** of this Affidavit.

3. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of the aforementioned violations are presently located at the SUBJECT PREMISES.

4. The following definitions apply to this Affidavit and Attachment B:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and e-mail.

b. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not

necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives,

“thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. “Geolocated,” as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A “hash value” is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a

computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. “Mobile application” or “chat application,” as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

o. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital,

anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

r. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

s. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3)(A)(i). Specifically, the United States District Court for the Western District of Oklahoma is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” *Id.*

### **BACKGROUND ON DISCORD**

6. According to Discord’s website and other open-source publications, Discord is an instant messaging and digital distribution platform. Discord allows users to communicate with voice calls, video calls, text messages, and other forms of digital media in private invite only chats or in communities. These communities are called servers and



are designed to group like minded users into social organizations revolving around a common interest.

7. The only requirement to create an account within Discord is to provide a valid e-mail address and to create a username. However, contrary to other popular applications, the username is not required to be unique. Once the user creates a username, Discord randomly assigns a “discriminator” consisting of a pound sign/hashtag followed by four numbers. It is possible to change your username and discriminator once a Discord account is created.

8. Discord collects and stores information voluntarily provided by the user onto Discord’s servers. This information includes information required to activate an account, such as e-mail address, and any messages, images, and other content sent via the chat feature. Other information collected and stored by Discord includes IP address, device ID, and user activities. Discord retains this information as long as it determines the information to be relevant.

9. When Discord discovers a user uploading Child Sexual Abuse Material (CSAM), Discord reports the user and user’s information to the National Center for Missing and Exploited Children (NCMEC). The user is then removed from Discord and the reported CSAM is removed from Discord’s servers.

### **PROBABLE CAUSE**

10. NCMEC is a non-governmental organization that, among other things, tracks missing and exploited children and serves as a repository for information about child pornography. Electronic Service Providers (ESPs), such as Discord, and internet service

providers (ISPs) are required by Title 18, United States Code, Section 2258A to report apparent child pornography to NCMEC's CyberTipline (CT) reporting system when they become aware of its existence. To make such a report, these ISPs and ESPs go to NCMEC's online portal and input information concerning the child exploitation activity it believes to have occurred, including the incident type, the incident time, any screen or usernames associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. Other than the incident type and incident time, the remainder of the information the ISP/ESP provides is voluntary and undertaken at the initiative of the reporting ISP and ESP.

11. The ISPs and ESPs may also upload to the NCMEC any files it collected in connection with the activity. Using publicly available search tools, the NCMEC then attempts to locate where the activity occurred based on the information the ISP or ESP provides, such as IP addresses. The NCMEC then packages the information from the ISP or ESP, along with any additional information it has such as previous related CTs and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

12. On April 06, 2021, NCMEC received a CT report from Discord regarding apparent child pornography. Discord provided an image file of apparent child pornography reportedly uploaded onto Discord servers by "LoneWolf#1303." The CT is detailed in NCMEC CT report number 88610216.

13. After receiving Discord's report, NCMEC provided CT report number 88610216 to the Oklahoma State Bureau of Investigation ("OSBI"), who then relayed the same to HSI Amarillo, Texas.

14. NCMEC CT 88610216 indicates that on March 25, 2021, 06:42:21 Universal Time Coordinated (UTC), a Discord user with username LoneWolf#1303 uploaded an image of apparent child pornography. The CT, based on information provided by Discord, indicates LoneWolf#1303 uploaded the image, with a file name of "image0-22.jpg," from IP address 67.219.169.152. The CT shows that Discord username LoneWolf#1303 is associated with e-mail address saritaswift123@gmail.com and ESP User ID 772504241733369857. The CT specifies that IP address 67.219.169.152 was geolocated in Guymon, Oklahoma. IP address 67.219.169.152 was provided for use by Internet Service Provider Panhandle Telecommunications Cooperative Inc. (PTCI).

15. I reviewed the "image0-22.jpg" which Discord provided to NCMEC in CT 88610216 and determined the image to be child pornography. The image depicts a pre-pubescent female performing oral-to-genital sex on an adult male. The prepubescent female's bottom half is unclothed, and her genitalia are exposed.

16. On April 12, 2021, NCMEC received an additional CT from Discord referencing user LoneWolf#1303 uploading apparent child pornography. The CT is detailed in NCMEC CT report number 88856550.

17. NCMEC CT 8886550 indicates that on March 28, 2021, 23:16:18 UTC, a Discord user with username LoneWolf#1303 uploaded a video, file name "VID-20191231-WA0039.mp4," of apparent child pornography. The CT indicates LoneWolf#1303

uploaded the video file from IP address 67.219.169.152. The CT shows that Discord username LoneWolf#1303 is associated with e-mail address saritaswift123@gmail.com and ESP User ID 772504241733369857. The CT specifies that IP address 67.219.169.152 was geolocated in Guymon, Oklahoma. IP address 67.219.169.152 was provided for use by Internet Service Provider PTCI.

18. I reviewed video file name "VID-20191231-WA0039.mp4" provided by Discord to NCMEC and determined the file to be child pornography. The file is a one minute and fifty-one second video which depicts genital-to-genital intercourse between an adult male and pre-pubescent female.

19. On April 28, 2021, I reviewed basic subscriber information for IP address 67.219.169.152, provided by PTCI through service of an administrative subpoena. The information provided listed RAFAEL MARTINEZ TAPIA; DOB: October 27, 1972, as the user of the aforementioned IP address on March 25, 2021 and March 28, 2021. Also returned was a physical and mailing address for RAFAEL MARTINEZ TAPIA of 1111 S. Ellison Street, Guymon, Oklahoma 73942. RAFAEL MARTINEZ TAPIA's service with PTCI started on May 25, 2016. PTCI last received a cash payment for service from RAFAEL MARTINEZ TAPIA on March 23, 2021. Additionally, PTCI advised the device used to access the IP address was a Calix brand router provided by PTCI to RAFAEL MARTINEZ TAPIA for being a WiFi service customer.

20. On May 12, 2021, I contacted the Texas County, Oklahoma Assessor's office for records related to 1111 S. Ellison Street, Guymon, Oklahoma. The Assessor provided a parcel map and account listing for parcel 700001943, the property where 1111 S. Ellison

Street was located. The parcel encompasses the entire block surrounded by S. Ellison Street, S.E. 11th Street, EO 235 Road, and South Crumley Street. The parcel consisted of 24 individual lots, all of which are owned by Gonzalez Escarcega Investments LLC (GEI).

21. On May 12, 2021, I contacted Jaime Gonzalez-Escarcega, a registered agent of GEI, regarding parcel 700001943 located in Guymon, Oklahoma. Gonzalez-Escarcega advised he owned the parcel and rented the lots to individual tenants. The tenants owned their respective mobile homes and paid a fee to GEI for use of the lot. Gonzalez-Escarcega stated the lot located at 1111 S. Ellison Street, Guymon, Oklahoma, has been rented by RAFAEL MARTINEZ and Ana Luisa Cerrano Montelongo since September 08, 2017. (RAFAEL MARTINEZ and RAFAEL MARTINEZ TAPIA are believed to be one-in-the same. Herein, MARTINEZ will be referenced as MARTINEZ TAPIA.) MARTINEZ TAPIA last paid \$200.00 towards his “lot rent” on May 05, 2021. Gonzalez-Escarcega provided a copy of the rental agreement between Gonzalez-Escarcega and MARTINEZ TAPIA, as well as a billing statement showing lot rental payments for 1111 S. Ellison Street, Guymon, Oklahoma, made by MARTINEZ TAPIA.

22. On May 18, 2021, I coordinated with Special Agent Joe Mosely, United States Postal Inspection Service (USPIS). SA Mosely was able to use resources available to him and advised a piece of mail addressed to “RAFAEL MARTINEZ [TAPIA],” was delivered by the United States Postal Service to 1111 S. Ellison Street, Guymon, Oklahoma, that same day.

23. On June 08, 2021, I received basic subscriber information for Discord User ID: 772504241733369857, provided by Discord through service of an administrative

subpoena. The information provided by Discord showed the account was registered on November 01, 2020, and at the time of process had been deleted. No verified e-mail was associated to the User ID.

24. Additional information provided by Discord was data related to IP address 67.219.169.152 accessing Discord's servers. This information was categorized as "Session Start" times in UTC. IP Address 67.219.169.152 started a session 37 separate times between March 25, 2021 and April 6, 2021. The end date of April 6, 2021 coincides with the report date of NCMEC CT 88610216 and Discord's policy of reporting Child Pornography to NCMEC and subsequent deletion of the offending account. Referencing previous investigative activities, NCMEC CT 88610216 and 88856550 showed IP Address 67.219.169.152 and User ID 772504241733369857 uploaded Child Pornography on separate occasions on March 25, 2021 at 06:42:21 UTC and March 28, 2021 at 23:16:18 UTC, respectively. Discord provided session start times for IP Address 67.219.169.152 on March 25, 2021 at 06:40:24 UTC and on March 28, 2021 at 23:11:51 UTC.

25. On June 29, 2021, I confirmed with PTCI that account information related to 1111 S. Ellison St., Guymon, Oklahoma, and IP address 67.219.169.152 had not changed. I also confirmed with GEI, who advised the same tenant was renting the lot at 1111 S. Ellison Street, Guymon, Oklahoma. Further coordination with NCMEC revealed seven additional CT associated to IP Address 67.219.169.152.

26. On July 13, 2021, while conducting surveillance of 1111 S. Ellison Street, Guymon, Oklahoma, I witnessed one male and one female exit the residence and enter a gray 2006 Chevrolet Impala, Oklahoma license plate EYH861, parked directly in front of

the residence. The male was heavy-set and appeared to be of Hispanic descent. The vehicle left the residence and travelled to the McDonald's restaurant located at 1906 Highway 64 N, Guymon, Oklahoma, where the female occupant exited the vehicle and went inside the restaurant. The male driver returned to the 1111 S. Ellison Street, Guymon, Oklahoma residence alone and exited the vehicle then entered the residence. On August 12, 2021, I witnessed the same male and female occupants of the 1111 S. Ellison Street, Guymon, Oklahoma residence exit the dwelling and enter a brown 2009 Buick Enclave, Kansas license plate 796NDN, parked in front of the home. The vehicle drove to the United States Postal Service mailbox cluster unit, checked the mail, then left the area. The vehicle, along with both occupants, returned approximately eight minutes later. The male and female gathered what appeared to be groceries from the vehicle and entered the residence.

27. On August 13, 2021, in an attempt to identify the female occupant of the residence, I conducted open source and law enforcement records checks for Pablo Ontiveros Serrano (USC), the registered owner of the vehicles in front of the 1111 S. Ellison St. Guymon, Oklahoma address. The checks revealed Pablo Ontiveros Serrano was born in Mexico on June 07, 1993 and immigrated to the United States in 2012 as a child of a Lawful Permanent Resident.

A check of Pablo Ontiveros Serrano's sponsor/parent revealed the principal applicant as Susana Serrano Montelongo (USC) born in Mexico on August 11, 1974. Susana Serrano Montelongo provided an address of 808 N Lelia St, Guymon, OK on her immigrant visa (IV) application. Also listed on her IV was a spouse, Guadalupe



Ontiveros Silva (USC), September 27, 1948, who resided at the same 808 N Lelia St, Guymon, Oklahoma address.

The picture attached to Susana Serrano Montelongo's IV application appeared to match the female entering and exiting the 1111 S. Ellison St residence witnessed through surveillance.

A review of photographs associated to Guadalupe Ontiveros Silva revealed he did not match the description of the male occupant of the 1111 S. Ellison St, address. Based on previous surveillance, the male occupant appeared to be younger than Ontiveros Silva. Open source records search for Ontiveros Silva showed a probable current address of 404 S. May St. Guymon OK.

28. Accordingly, I believe electronic devices capable of accessing the internet and/or storing digital content, to include personal computers and any smartphones will be located at the SUBJECT PREMISES. As described above, I believe contraband and evidence, fruits, and instrumentalities of the aforementioned violations are presently located at the SUBJECT PREMISES.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE  
INTERNET**

29. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers



serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “Wi-Fi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which plug into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video

with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Individuals can easily store, carry, or conceal media storage devices on their persons. Individuals also often carry smartphones and/or mobile phones.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where an individual uses online storage, however, law enforcement can find evidence of child pornography on the user’s computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as “apps.” Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact

directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored. Files stored on one smartphone can be easily transferred to another phone by using a SIM card. Moreover, the same files can be simultaneously stored on multiple smartphones and other computers. Thus, I am requesting to seize all computers of individuals identified as residing in the SUBJECT PREMISES, to include: cellular devices, tablet type computers, and other devices capable of storing electronic data not specifically named at the SUBJECT PREMISES—not any specific computer. Devices belonging to individuals identified as mere guests will not be subjected to seizure or search.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information such as the traces of the path of an electronic communication may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information exists indefinitely until overwritten by other data.

**CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

30. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access, receive, possess, distribute, produce, and/or collect child pornography:

i. Child pornography collectors usually start collecting child pornography by obtaining free images and videos of child pornography widely available on the internet on various locations and then escalate their activity by proactively distributing images they have collected, often for the purposes of trading images of child pornography with others, as a method of adding to their own collection of child pornography.

j. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

k. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the

inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

l. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years. Collectors prefer not to be without their child pornography for any prolonged time period.

m. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the collector to view the collection, which is valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

n. Child pornography collectors also may correspond with and/or meet others to share information and materials; keep correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

o. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.<sup>1</sup>

p. Even if MARTINEZ TAPIA uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

q. In light of the aforementioned, including the facts that demonstrate MARTINEZ TAPIA possessed and distributed child pornography in a Discord chat forum, based on my training and experience, I believe that it is probable that MARTINEZ TAPIA is a child pornography collector.

### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

31. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and

---

<sup>1</sup> See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

r. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

s. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

t. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

u. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file, which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

32. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system’s input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified



computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

v. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

w. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

33. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is

equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

#### **BIOMETRIC ACCESS TO DEVICES**

34. I request that this warrant permit law enforcement to compel MARTINEZ TAPIA to unlock any electronic devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

x. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint

scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

y. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

z. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

aa. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

bb. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

cc. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the electronic devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the electronic devices,

making the use of biometric features necessary to the execution of the search authorized by this warrant.

dd. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, certain Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for eight hours and the passcode or password has not been entered in the last six days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

ee. Due to the foregoing, if law enforcement personnel encounter any electronic devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of MARTINEZ TAPIA to the fingerprint scanner of the electronic devices found at the SUBJECT PREMISES; (2) hold the devices found at the SUBJECT PREMISES in

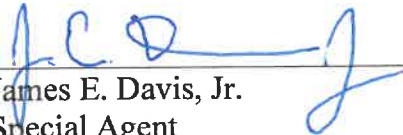
front of the face of MARTINEZ TAPIA and activate the facial recognition feature; and/or (3) hold the devices found at the SUBJECT PREMISES in front of the face of MARTINEZ TAPIA and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to require that MARTINEZ TAPIA state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to require MARTINEZ TAPIA to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

### **CONCLUSION**


35. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the location described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

36. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return”

inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

  
James E. Davis, Jr.  
Special Agent  
Homeland Security Investigations

Subscribed and sworn before me this 18th day of August, 2021 and I find probable cause.

  
SUZANNE MITCHELL  
United States Magistrate Judge

**ATTACHMENT A**

**DESCRIPTION OF LOCATIONS TO BE SEARCHED**

The entire house, curtilage, appurtenances, and vehicles parked at the single-family residence described as: 1111 S. Ellison Street, Guymon, Oklahoma. The residence is a mobile home/trailer home. The residence is a light brown color with dark brown trim along the roofline. The residence is located in a row of mobile homes. The numbers "1111" can faintly be seen painted on the North West corner of the residence. Additional numbering of "1111" is attached to the same North West corner of the residence directly above the faded painted numbers. A decoration of a pink flower and pink and yellow butterfly are attached to the residence just below the "1111" markings. A metallic frog decoration is also affixed to the side of the residence adjacent to the "1111" markings.





**ATTACHMENT B**

**ITEMS TO BE SEIZED AND SEARCHED**

The following materials, that are the property of the residents of 1111 S. Ellison St., Guymon Oklahoma or are in the constructive possession of the residents to exclude items belonging to temporary visitors, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 USC § 2252A (Possession, distribution, and receipt of child pornography):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well

as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet

search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of internet applications;

e. Records and information showing access to and/or use of internet applications related to the sexual exploitation of children; and

f. Records and information relating or pertaining to the identity of the person

or persons using seized evidence.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.